Vragen en antwoorden die zijn gesteld aan en gegeven door deskundigen op het terrein van de Common Criteria

Vraag 1
Wat is het gangbare proces om het juiste EAL-niveau te kunnen bepalen?

Antwoord
De klassieke weg om dit vast te stellen is door te bepalen wat het potentieel is van de aanvaller waartegen de systemen moeten zijn beveiligd met inachtneming van de mate waarin vertrouwd kan worden op de omgeving waarin de stemprinter en stemmenteller zullen worden gebruikt. Gelet op het belang dat verkiezingen vertegenwoordigen zou voor de stemprinter en de stemmenteller uitgegaan moeten worden van een "high attack potential" aanvaller. Dat plaatst de systemen gelijk in het domein van de EAL 6 (high attack potential). EAL 5 gaat immers uit van een "enhanced moderate attack potential". Verder kan er niet vanuit worden gegaan dat er beschermende maatregelen zijn te nemen die uitsluiten dat een iemand met een "high attack potential" de beschikking krijgt over een stemprinter of stemmenteller. Die persoon of organisatie zou dan kunnen aantonen dat de beveiliging niet voldoet. Dat kan potentieel politiek en maatschappelijk leiden tot verlies aan vertrouwen in de betrouwbaarheid van de stemprinter en stemmenteller. Het bieden van bescherming tegen een dergelijke aanval is een lastige taak. Er kunnen echter in deze context bijvoorbeeld inbraakdetectie methoden worden gebruikt die bescherming bieden tegen een bedreiging. Een alternatieve benadering zou zijn om te kijken naar de details van elke EAL en te beslissen of elk aspect dat is vervat in een EAL relevant is of niet.

Beide benaderingen worden ook vaak gecombineerd. In eerste instantie leidt de algemene beslissing over het aanvalspotentieel tot een basale EAL. Vervolgens wordt elk aspect van de EAL bekeken en aangevuld (of verwijderd) waar nodig geacht. Dit leidt vaak tot de tussenliggende niveaus van EAL X +.

Vraag 2
Is gebruik van standaardcomponenten mogelijk bij een EAL-niveau van 5 en 6?

Antwoord
Het is een bijna onmogelijke opgave om gebruik te kunnen maken van standaardcomponenten. Allereerst omdat de meeste standaardcomponenten niet ontwikkeld zijn om bestand te zijn tegen een "high attack potential" aanval. Daarnaast moet bij EAL 5 en 6 nauwgezet worden gedocumenteerd hoe de apparatuur en de programmatuur precies is samengesteld, hoe het is gefabriceerd en hoe het werkt. Dat is bij de ontwikkeling van standaardcomponenten niet gebeurd. Voor een EAL 5 of 6 certificering zou voor de betreffende componenten dat werk alsnog gedaan moeten worden. Het risico is groot dat de leverancier er niet goed in slaagt en daardoor dus ook niet door de certificering komt.

Gewezen wordt op de ervaringen met de certificering van betaalautomaten. In het verleden werden voor deze systemen weinig of geen standaardcomponenten gebruikt en was als gevolg hiervan de beveiliging van een hoog niveau. Door allerlei commerciële ontwikkelingen zijn leveranciers daarvan afgestapt en worden er standaardcomponenten gebruikt. Als gevolg hiervan is bij certificeringstrajecten vastgesteld dat het beveiligingsniveau lager is en de betaalautomaten gevoeliger zijn geworden voor dreigingen.

Voor de stemprinter is, zo heeft de commissie Van Beek geoordeeld, cruciaal dat de keuze die de kiezer maakt niet wordt opgeslagen nadat die keuze is geprint. Dit is met standaardcomponenten naar alle waarschijnlijkheid niet te realiseren. Immers van standaardcomponenten is niet beschreven hoe ze precies werken en waar, wanneer, wat wordt opgeslagen.

Hierbij dient te worden vermeld dat deze beperkingen alleen gelden voor de aspecten van de apparaten die relevant zijn voor de beveiliging. Wanneer standaard hardware of software wordt gebruikt in delen van het apparaat die niet relevant zijn voor de beveiliging, dan richt de beoordeling zich niet op deze delen. Een standaard CPU (zonder enige vorm van crypto) is een voorbeeld van een dergelijk generiek onderdeel. Gewoonlijk wordt aangenomen dat deze onderdelen betrouwbaar zijn, zonder dat gedetailleerde informatie over die componenten beschikbaar dient te zijn. De beslissing wat wel of niet relevant is voor de beveiliging is niet makkelijk te nemen en leidt derhalve tot discussies.

Vraag 3
Wat is het verschil tussen EAL 4, 5 en 6?

Antwoord
Tot EAL-niveau 4 worden de vereisten steeds strenger en meer gedetailleerd, maar worden geen zeer gespecialiseerde technieken op het gebied van beveiligingsengineering vereist. EAL1-4 kunnen over het algemeen worden gebruikt voor de modificatie van reeds bestaande producten en systemen. Boven niveau EAL4 wordt een toenemende mate van toepassing vereist van gespecialiseerde technieken op het gebied van beveiligingsengineering. Om ervoor te zorgen dat systemen voldoen aan de vereisten van deze niveaus, moeten ze zijn ontworpen en ontwikkeld met de intentie om aan die vereisten te voldoen.

Een EAL4-evaluatie biedt, naast EAL3, een analyse die wordt ondersteund door een volledige specificatie van de interface, een beschrijving van het modulaire basisontwerp van de TOE (Target of Evaluation) en een subset van de implementatie. Het testen wordt ondersteund door een analyse van de kwetsbaarheid (waarbij ook gebruik wordt gemaakt van de implementatie-representatie), waarmee de weerstand wordt aangetoond tegen aanvallers met een aanvalspotentieel dat hoger is dan basaal. Waarborging wordt ook geboden via aanvullend geautomatiseerd configuratiemanagement.

EAL5 is van toepassing wanneer een hoge mate van onafhankelijk gewaarborgde beveiliging is vereist, met een robuuste aanpak van de ontwikkeling. Een EAL5-evaluatie biedt, naast EAL4, een analyse die wordt ondersteund door een modulair ontwerp van de beveiligingsfuncties van de TOE. Waarborging wordt aangevuld met een semi-formele presentatie van het ontwerp, een gestructureerde architectuur, uitgebreid configuratiemanagement van de TOE en een onafhankelijke, methodische analyse van de kwetsbaarheid waarmee de weerstand wordt aangetoond tegen aanvallers met een matig aanvalspotentieel.

Een EAL6-evaluatie biedt, naast EAL5, aanvullende waarborging door middel van een formeel model van het beveiligingsbeleid van de TOE en een semi-formele presentatie van de functionele specificatie en het ontwerp van de TOE (Target of Evaluation). De onafhankelijke, methodische analyse van de kwetsbaarheid toont de weerstand aan tegen aanvallers met een hoog aanvalspotentieel.

Samenvattend: het verhogen van het waarborgingsniveau zorgt ervoor dat de maatregelen die worden toegepast vollediger zijn (de controles gaan van een subset naar een volledige set). Dit leidt ook tot het gebruik van meer (semi)-formele methoden. Met name het gebruik van (semi)-formele methoden heeft een aanzienlijke invloed op zowel de ontwikkeling van het product als de evaluatie ervan.

Vraag 4
Kunnen procedurele maatregelen meetellen als beveiligingsmaatregelen in een evaluatie voor EAL 5 en 6?

Antwoord
Het Common Criteria-systeem gaat uit van de veronderstelling dat het product cq systeem dat moet worden geëvalueerd (TOE) werkt binnen een specifieke omgeving die bijdraagt aan de beveiligingskenmerken van het totale product cq systeem. Dat zou een probleem kunnen vormen voor de stemprinter en stemmenteller, aangezien men slechts een zeer beperkt vertrouwen kan hebben in de omgeving. Dat probleem begint al bij de ontwikkelaar. Uitgaande van het stelsel van de Common Criteria zou de ontwikkelaar vertrouwd moeten worden.

Echter voor het verkiezingsproces is dat al een stap te veel. Ook de ontwikkelaar kan een dreiging opleveren voor de integriteit van de systemen. Het complicerende hier is de politiek/maatschappelijke context. De systemen moeten niet alleen beveiligd zijn tegen daadwerkelijke dreigingen, maar ook tegen het feit dat er personen en/of groeperingen kunnen zijn die zich inzetten om aan te tonen dat de systemen bedreigd kunnen worden. Dat maakt deze casus extra complex. Dit leidt tot een situatie waarin de klassieke maatregelen van een Common Criteria-beoordeling niet voldoende zijn, maar mogelijk moeten worden aangevuld met specifieke eisen binnen of buiten de Common Criteria-beoordeling.

Vraag 5
Zou met procedurele maatregelen een lager niveau dan EAL 5 of 6 kunnen volstaan?

Antwoord
Zie het antwoord op vraag 4. Het stelsel van Common Criteria kent de mogelijkheid om een EAL niveau te kiezen (bijvoorbeeld EAL 4) en vervolgens (als zogenaamde "plussen") een aantal maatregelen van toepassing te verklaren uit de hogere niveaus (bijvoorbeeld EAL 5 en/of 6). Procedurele maatregelen, zoals bijvoorbeeld een visuele controle van een (relatief klein) deel van de elektronisch getelde papieren stembiljetten is een maatregel op basis waarvan zou kunnen worden geoordeeld dat de TOE een minder hoog beveiligingsniveau zou kunnen hebben. De vraag die dan beantwoord moet worden is hoe groot de kans is dat met een dergelijke visuele controle van een (relatief klein) deel van de elektronisch getelde papieren stembiljetten daadwerkelijk kan worden opgespoord dat stemmentellers niet correct hebben gewerkt. Als de kans daarop niet groot is, dan zou nog steeds sprake moeten zijn van een "high attack potential".

Ook een visuele controle door de kiezer van diens geprinte stemkeuze kan niet als dekkend worden beoordeeld, omdat zeker niet alle kiezers die controle zullen uitvoeren. Zou het voorkomen dat de stemprinter iets anders geprint heeft dan de keizer heeft beoogd en dit is reproduceerbaar dan zal wederom het vertrouwen in de betrouwbaarheid van de stemprinter in het geding zijn.

De beveiligingsmaatregelen die worden geboden door de TOE en de maatregelen die worden geboden door de omgeving dienen met zorg te worden vastgesteld. Hierbij dient niet de vraag leidend te zijn hoe de last van het certificeringsproces kan worden beperkt. Leidend voor de te nemen beveiligingsmaatregelen moet een diepgaande analyse van de dreigingen zijn.

Vraag 6
Is het mogelijk en haalbaar om een stemprinter en stemmenteller te ontwikkelen die voldoet aan EAL 5 of 6?

Antwoord
Ja, mits de leverancier die deze systemen gaat ontwikkelen ervaring heeft met het ontwikkelen van producten van een niveau van EAL 4 of hoger. Er bestaat een aanzienlijk risico dat de ontwikkeling en evaluatie/certificering zal mislukken indien een leverancier die ervaring niet heeft.

Vraag 7
Hoeveel tijd moet gerekend worden voor de ontwikkeling van een stemprinter en stemmenteller op EAL 5 of 6 niveau?

Antwoord
Meer dan een jaar moet verwacht worden. Het hangt onder meer af van de specificaties van de systemen en van de ervaring van de leverancier en tenslotte van de ervaring van de evaluator. Van EAL 1 tot en met 4 neemt de extra inspanning voor het toepassen van de CC nog lineair toe, vanaf niveau 5 neemt die extra inspanning exponentieel toe dankzij het gebruik van (semi)formele methodes.

Vraag 8
Geef een toelichting op het aanvalsniveau dat bij een EAL hoort.

Antwoord
Om het dreigingsniveau te kunnen bepalen waartegen een systeem moet zijn beveiligd maakt de CC gebruik van een classificatiemethode waarbij aan een bepaalde aanval een bepaald aantal "punten" wordt toegekend. De volledige methode wordt beschreven in bijlage "B.4 Calculating attack potential". Een aanval met een cijfer tussen de 20 en 24 wordt bijvoorbeeld geclassificeerd als "Hoog". Dit betekent dat een aanvaller met aanvalspotentieel "hoog" in staat wordt geacht deze te kunnen uitvoeren, maar een aanvaller met aanvalspotentieel "matig" of lager niet. Hierbij dient te worden opgemerkt dat wat betreft de betrokken factoren, het aanvalspotentieel van een aanvaller afhankelijk kan zijn van een specifieke combinatie van deskundigheid en apparatuur. Een laboratorium gespecialiseerd in bepaalde aanvallen op internetprotocollen en -toepassingen kan bijvoorbeeld een hoog aanvalspotentieel hebben met betrekking tot webservers maar geen hoog aanvalspotentieel met betrekking tot aanvallen op smartcards.

Hieronder is samengevat weergegeven welk aanvalspotentieel aan een EAL wordt toegekend. De beschrijving van het aanvalspotentieel verwijst hier altijd naar het niveau van een aanvaller waartegen de TOE bestand moet zijn. Met andere woorden: Voor een aanvaller op dit niveau mag het NIET mogelijk zijn om een aanval uit te voeren op de mogelijk resterende kwetsbaarheden.

- **EAL 7 en 6: Hoog/High**

Een civiel beveiligingslab of een georganiseerde groep hackers of een universitair team gespecialiseerd in de technologie die wordt gebruikt in het product.

- **EAL 5: Matig/Moderate**

Beveiligingsexperts (door leken "hackers" genoemd, hoewel sommige "hackers" mogelijk een hoger deskundigheidsniveau hebben).

- **EAL 4: Hoger dan basaal/Enhanced basic**

Personen die beschikken over IT-vaardigheden op een bepaald technologisch gebied, maar niet gespecialiseerd zijn in het zoeken naar kwetsbaarheden.

- **EAL 3 en lager: Basaal/basic**

Personen die geen specifieke vaardigheden of kennis bezitten en zich alleen richten op algemeen bekende kwetsbaarheden, of in aanvulling daarop willekeurige pogingen doen om kwetsbaarheden te vinden. Als het gaat om internettechnologie vallen bijvoorbeeld de zogenaamde "script-kiddies" in deze categorie, ofwel personen die gebruik maken van gepubliceerde hulpmiddelen voor de aanval op kwetsbaarheden zonder deze kwetsbaarheden noodzakelijkerwijs te begrijpen.

Vragen die zijn gesteld en antwoorden die zijn gegeven door deskundigen op het terrein van de ontwikkeling van apparatuur

Vraag 1
Hoe ziet een ontwikkeltraject waarbij (ook) hardware moet worden ontworpen en ontwikkeld in elkaar? Wat moet, in de vorm van eisen, bekend zijn voordat begonnen kan worden met ontwerpen en ontwikkelen van hardware?

Antwoord:
In wezen niet anders dan bij een "regulier systeemontwikkeltraject". Dat wil zeggen dat de opdrachtgever idealiter op functioneel niveau specificeert wat er moet worden ontwikkeld en welke randvoorwaarden gelden. De leverancier vertaalt die specificaties en maakt, waar de specificaties dat toestaan, nadere keuzes. Idealiter zou je willen dat het specificeren van de eisen door de opdrachtgever in samenspraak kan plaatsvinden met de leveranciers.

Het ontwerp- en ontwikkeltraject van complexe hardware/software-systemen verloopt in het algemeen het beste als de opdrachtgever continu betrokken is in het proces. Een co-development verhoogt in dit soort projecten de kans op succes. Zo is het vaak bij het analyseren van de eisen door de opdrachtnemer zinvol om de achterliggende gedachte van een eis te kennen. Bepaalde eisen kunnen grote impact hebben op kosten en/of complexiteit, terwijl het achterliggende doel ook op andere manieren behaald kan worden. Dit tegen lagere kosten of een eenvoudiger concept.

Een goede dialoog met de opdrachtgever is dus zinvol om een kosteneffectieve en de minst complexe oplossing te realiseren met behoud functionaliteit. Daarom wordt erop geattendeerd dat het van belang is om voorzichtig te zijn in het formuleren van de specificaties. De slag die het Ministerie en de Commissie nu maken in de vertaling van het gekozen kiesproces naar functionele eisen is vooral van groot belang in het opstellen van een passend Protection Profile, omdat dat immers de impact op de Common Criteria evaluatie heeft. Als voorbeeld wordt genoemd: niet specificeren "alles moet worden verwijderd uit het geheugen", maar "uit het geheugen moet de informatie over de keuze van de kiezer worden verwijderd". Verder is van belang wanneer de keuze van de kiezer verwijderd moet worden. Is dat onmiddellijk nadat de kiezer de keuze heeft gemaakt of kan dat later zijn. Verder is aangegeven dat in een gecombineerd ontwikkeltraject met software en hardware er kruisverbanden liggen tussen de keuzes in de hardware en de software. Het aanpassen van de eisen en ontwerpkeuzes na de initiële designfase kunnen van grote invloed zijn. Dit kan leiden tot inefficiëntie en vertragingen.

Een onderwerp waar relatief veel over gesproken is in het overleg, is het wissen van het geheugen op de stemprinter. Het verwijderen van keuzen uit geheugens van de stemprinter kan bijvoorbeeld door meermaals overschrijven van het geheugen of door de stroom van componenten met geheugen af te halen. Geheugen wissen door stroom van componenten af te halen werkt echter alleen voor tijdelijk geheugen en niet voor permanent geheugen, zoals een harde schijf of flash memory. Daarnaast moet de stroom er lang genoeg afgehaald worden, zodat zeker is dat alle sporen van hetgeen is opgeslagen zijn verdwenen. Het op geautomatiseerde wijze afschakelen van de stroom van een component vergt maatwerk aan de component. Die "functionaliteit" is namelijk niet standaard. Het is de vraag of dit een geaccepteerde methode is volgens de Common Criteria evaluatoren, wat weer afhangt van de verwoording van de eis tot wissen van het geheugen in het Protection Profile.

Daarnaast zal het tijd duren voordat de component, nadat deze is aangezet, weer operationeel is. Gezien voorgaande consequenties zal het overschrijven van het geheugen veelal simpeler zijn, mits de werking van het gebruik van het geheugen is gedocumenteerd. Als dit allemaal in ogenschouw wordt genomen, dan is het aannemelijk te concluderen dat overschrijven van geheugen veelal simpeler zal zijn, mits precies is gedocumenteerd hoe het geheugen wordt gebruikt. Het is niet waarschijnlijk dat dit laatste bij standaardcomponenten het geval zal zijn.

De verwachting is dat aan- en uitzetten van componenten, gezien het aantal keer dat een stemprinter voor het maken van een stemkeuze wordt gebruikt (rond de 1000 per verkiezing), geen significante invloed zal hebben op de levensduur. Vanzelfsprekend zal dit in de componentkeuze geverifieerd moeten worden.

Vraag 2
Heeft het feit dat de hardware wordt ontwikkeld gevolgen voor de ontwikkeling van de software waar de hardware gebruik van gaat maken? Gedacht zou kunnen worden aan gevolgen voor de te hanteren ontwerpmethode, de te gebruiken ontwikkelomgeving, de te gebruiken programmeertalen, de wijze van testen, de te gebruiken testhulpmiddelen en het proces van het installeren van de software op de hardware.

Antwoord:
Neen. De wijze waarop de software wordt ontwikkeld en getest is niet anders dan bij standaard elektronica die ingekocht wordt. Wel zal om aan de Common Criteria eisen te kunnen voldoen gewerkt moeten worden met een volgens Common Criteria geaccepteerde of accepteerbaar te maken programmeertaal en ontwikkelomgeving. Voor de goede orde is het daarbij goed om te melden dat windows/android/java en andere veelgebruikte commerciële omgevingen vrijwel per definitie niet geschikt zijn om te gebruiken om een te certificeren systeem op te baseren ivm EAL5/6-eisen. Datzelfde geldt voor de typische hardware waar dit soort systemen op draait, zoals intel- en AMD-processoren. (Waarbij de kanttekening gemaakt moet worden dat daar waar de hardware component niet kritisch is voor de beveiliging, dit wel een standaard component mag zijn. Het is aan de evaluatoren om uiteindelijk te bepalen of een systeem onderdeel kritisch is voor de beveiliging of niet.) Hieronder valt dat de evaluator inzage moet hebben in alle programmatuur. Het gebruikmaken van standaard programmabibliotheken is lastig in dit geval. Een aantal programmeertalen en –compilers zou voor de hand kunnen liggen om te gebruiken, zoals assembly, de programmeertaal van de processor ook wel machine taal genoemd, C of C++. Maar deze lijst is niet uitputtend.

Naast de taal en compiler is de grootste impact van Common Criteria certificering op de systeemontwikkeling dat er veel meer eisen gesteld worden aan het ontwerpproces en de ontwerpers in termen van documentatie, screening en locatie.
Overigens is in het (denkbeeldige) geval dat er met standaard hardware gewerkt zou gaan worden geen grote kostenbesparing te verwachten in het gehele traject, omdat het samengestelde systeem van hardware en software, uiteindelijk als geheel ontworpen, ontwikkeld en gecertificeerd zal moeten worden.

Vraag 3
Wat zijn de gevolgen ten aanzien van de doorlooptijd, de kosten en de risico's voor een ontwikkelingstraject van een systeem als voor delen of voor het geheel van dat systeem de hardware moet worden ontworpen en ontwikkeld?

Antwoord:
De doorlooptijd die de commissie Van Beek heeft vermeld in het rapport (6 a 9 maanden) is niet reëel. Kijkend naar wat de systemen (stemprinter en stemmenteller) moeten kunnen is een doorlooptijd van minimaal 18 maanden te verwachten wanneer er geen CC eisen worden opgelegd. Wanneer er ook nog aan een CC EAL5 evaluatie moet worden voldaan is een doorlooptijd van enige jaren te verwachten. Voor het ontwerpproces van producten op EAL5/6 zijn moderne ontwikkeltechnieken als *Agile* en *Scrum* waarschijnlijk niet toepasbaar. In deze technieken wordt zeer flexibel omgegaan met o.a. wijzigingen in specificaties en documentatie. Voor EAL5/6 is juist een formele aanpak vereist en is dus een meer traditioneel waterval of V-model geschikt. Hierbij worden gestructureerd stap-voor-stap de functionele eisen in een aantal stappen vertaald in detail-eisen, waarna ze even gestructureerd worden omgezet in een product.

Vraag 4
Is het EAL-niveau waartegen de CC-evaluatie moet plaatsvinden van invloed op het antwoord op vraag 3? Zo ja, is dat te kwantificeren in tijd, kosten en risico's?

Antwoord:
Ja. Vanaf EAL niveau 5 moet er al rekening mee worden gehouden dat hardware, maar ook software, "op maat" gemaakt zal moeten worden om aan de CC eisen te kunnen voldoen. Hoe hoger het EAL-niveau, hoe stringenter de eisen aan het ontwerptraject, documentatie en testen zijn. Ook moet de evaluator meer doen tijdens het ontwerp-, ontwikkel- en testproces wat gaandeweg het traject waarschijnlijk zal leiden tot meer aanpassingen van het ontwerp en in de te ontwikkelen hardware. Concreet betekent dit dat naar mate het EAL niveau hoger wordt, er meer ontwikkeliteraties nodig zijn voordat het systeem succesvol gecertificeerd is.
Voor een harder antwoord op vragen 3 en 4 is meer onderzoek nodig. Een kosten- en tijdinschatting voor een dergelijk complex traject kan slecht gegeven worden zonder goed te doordenken wat eisen en oplossingen zijn.